Global Business & Development Law Journal

Volume 17
Issue 1 *Symposium Bordering on Terror Global Business in Times of Terror -- The Legal Issues*

Article 11

1-1-2004

Panel One: Unfunding Terror -- Perspectives on Unfunding Terror

Steve Zelinger
Solidus Networks, Inc., d/b/a Pay By Touch.

Commentary by Steve Zelinger*

Good morning. We are facing challenges arising from the coalescence of a number of historical facts creating problems that we never have had to deal with at the same time. We have seen a rise in global terrorism and a rise in virtual transactions—that is to say, non-paper transactions, whether they are for commodities or services; for example, telephone and Internet transactions. Then, of course, there is the ancient "Hawalla" system of virtual transactions in the Middle and Near East of which we have been reading much recently, which also escapes paper-based documentation. There has been a vast expansion of global business and personal transactions. I would be surprised if some of you had not transferred money via one of the private email money-transfer systems using your credit or debit cards.

At the same time, individuals in our societies are more concerned about personal privacy than ever. In the United States, there are federal and state regulatory structures covering privacy matters. Europe's privacy regimes are even more rigorous. In addition to these legal realities, businesses increasingly must address the brand and business implications of privacy, because a business might be doing something that is entirely legal but is so repugnant to its clients or customer base that, as a practical matter, the practice might show it down.

The consequent increase in regulations on business arising from these various problems raises costs and enlarges bureaucracy. Business, like government, does not currently have the bureaucracies to deal with the immensity of problems. It is estimated that the business sector will face an increase of about thirty to sixty percent in legal and regulatory costs in order to comply with new regulations arising from the USA PATRIOT Act, Sarbanes-Oxley, and other financial regulations that apply to what used to be called, "highly regulated institutions." Today, there is very little distinction between what used to be called a "highly regulated institution" and a non-regulated institution. Any business with global or transnational transactional capacity is now going to be regulated and will encounter the same kinds of costs.

Banks, for the most part, were used to reacting to such regulatory changes. Banks have the essential bureaucracy and framework enabling them to quickly adapt and comply with new requirements, notwithstanding the cost. The new regulations, by definition, however, apply to all kinds of institutions, both bank and non-bank, including the credit card companies. Facing this new regulatory structure was among my responsibilities when I was at VISA. This morning, I would like to take a few moments to discuss the challenges we faced—challenges which undoubtedly are exemplary of those faced by the business community in general.

---

* Former Senior Vice President, Senior Counsel, and Global Director of Litigation and Regulatory Affairs, Visa International; U.S. Dept. of Justice, Washington, D.C. Currently, General Counsel, Solidus Networks, Inc., d/b/a Pay By Touch.

The opinions stated here are personal and do not represent or bear upon the official positions of VISA International, VISA USA, or any VISA entity or VISA members.

VISA is a membership association comprised of about 21,500 financial institutions around the world. It constitutes a cross-border network or railroad between these institutions. When, for example, a cardholder who is traveling abroad uses a VISA card or MasterCard in another country, his or her home account is debited and a credit statement created in another country. The card association provides the connection between the two different banks. In the past, for purposes of such transactions, card associations really had no interest in knowing the specific identity of individual cardholders. Each account was essentially a card number attached to a credit rating, and the bank issuing the card had to guarantee the ability of the cardholder to cover the cost of a particular transaction. Now, the government is asking card associations and other companies to capture and attach a name, gender, race, or ethnicity to that card number. This development has created difficult issues for business. Based on my personal perspective and experience, I can tell you that this has left the business sector scurrying.

Even assuming creation of the necessary business bureaucracies, full compliance with all new regulatory and security requirements, and the collection and storage by the business sector of all this information, who is going to do something with it? Who can collate it? Who can restore it? Who can analyze it? The National Security Agency (NSA) is probably among the world's largest collectors of information. It has been suggested that the best the NSA can do is to analyze a mere two percent of the data it collects on a daily basis. If the NSA, whose purpose is the collection and analysis of such data, can only analyze about two percent of the data it collects, you can understand the difficulty for the business sector—generally speaking, business simply is not equipped to analyze this kind of data. Ultimately, what we are doing is leveraging the cost of doing business against the potential threat created by terrorism in our society. For example, the idea is that if you impose long lines and onerous regulations upon people traveling in our airports, the door through which terrorists can operate will be narrowed and, hopefully, closed. The analogy applies to the financial sector as well.

The post-September 11th changes in the legal and regulatory framework of the nation, resulted, among other things, in the IRS' being folded in with the intelligence and enforcement agencies to provide larger data collection units that could be accessed simultaneously. Thus, for a variety of reasons, September 11th motivated the IRS to become more active. One of the first things it did was to look at the credit card companies. The rise in terrorism gave the IRS a new interest in addressing the phenomenon of putative U.S. taxpayers who park their money outside of the United States while living on their debit or credit cards within the United States or abroad, in an effort to escape U.S. tax laws. Statements in court by the IRS suggest that tax-avoidance was of immediate concern; however, the IRS also was concerned that many of these same people may be engaging in money laundering and other financial transaction regulatory-avoidance schemes. The IRS has publicly commented that this type of activity costs the U.S. Treasury somewhere between seventy-five and one hundred fifty billion dollars a year.

In the months following September 11th, the IRS issued upon the credit card companies certain "John Doe Summonses." It is estimated that these were the largest single subpoenas or summons issued by the United States government since its inception. These summonses sought information for cardholders in sixty-one different countries who might engage in some kind of transaction with the United States. The breadth of the requests was breathtaking; for example, given the nature of the Internet, any non-U.S. resident buying a book over the Internet from a U.S.-based company would technically be transacting with the United States. Like the other card companies, which generally are organized to recognize a customer by card number and the financial institution that issued the card, VISA had a difficult time determining which data within its system would effectively respond to the request.

Certainly, the first difficulty was that member banks from among sixty-four different countries own the VISA system. Secondly, what data was Visa in a position to provide? Here we had a lawful summons, issued under U.S. statutes, confirmed by a U.S. court, that was imposed upon a U.S. business residing in the United States. And, since VISA is everywhere you want to be, it did not have a defense that it was not subject to the personal or subject matter jurisdiction of the United States. How was VISA going to respond to these lawful U.S. government requests without tripping over the privacy regimes of the European Union, Commonwealth Countries, OECD, and the hoary bank-privacy regulations of such countries as Luxembourg and Switzerland—two of the sixty-one jurisdictions whose cardholder information was requested? One can imagine that neither Swiss authorities, nor those of Luxembourg, the Isle of Man, Malta, Cypress, Gibraltar or other traditional financial sanctuaries were excited at the prospect of having their cardholders' data examined by the IRS. So VISA and the other card companies had to address that issue.

Next, it was determined that facial compliance with the IRS requests could take VISA approximately seven to nine years at a cost of ninety billion dollars to collate the information and put it in a form that was readable. That was a very difficult task and obviously not do-able. Again it came down to leveraging the kinds of information that was responsive to the court-ordered requests of U.S. government authorities relative to the costs.

VISA also had to face brand and consumer concerns. One can assume that most cardholders in the United States and abroad are not excited about having their card issuing institution assist the government in looking over their shoulder at what transactions they might have engaged in. The Right to Financial Privacy Act, which imposes upon U.S. banking institutions obligations to notify a banking client or depositor of an investigation of that depositor so that he or she can come forward and assert his or her rights, is specifically excepted and excluded by the statutes under which the John Doe Summonses were issued. Although the process of responding to the summonses essentially was to be anonymous, the credit card companies and banking institutions nonetheless had to worry about brand damage. After all, the fact of the John Doe Summonses and

their judicial enforcement by a federal court in Miami was public information. For example, what was to keep a VISA cardholder in Switzerland from switching to American Express or MasterCard—also the recipients of such summonses—if he or she were to believe that Amex or MasterCard would put up more of a fight against IRS regulations than might VISA? Nothing. One could easily lose market share were that to happen. These are the kinds of brand and business implications arising from, but going well beyond the legal limits of, the new regulatory structure, that businesses increasingly must deal with every day.

Another area of difficulty for financial institutions are the enhanced "know-your-customer" requirements of the USA PATRIOT Act. The Act, for example, imposes upon financial institutions additional requirements to know exactly who is sending a money order, who is receiving deposits, et cetera. Compliance is made all the more difficult with the increase of both Internet transactions and credit card transactions done merely by virtue of a PIN or account number. In a regulatory environment that is more gray than black-and-white, banks and other financial institutions are scurrying to figure out how they can and should comply. A number of international banks, for example, have established entirely new anti-money laundering units in an effort to comply with the regulations.

The ever-increasing responsibility put on business has created other problems. For example, are credit card and other non-depository financial services companies that historically have not been subject to the Truth and Lending Act, to come within its purview as a result of the USA PATRIOT Act? If so, what will the increased regulatory costs do to the cost of your credit or debit card transactions?

A potential concern for consumers is the discovery, by law enforcement and intelligence agencies, of the kind of data that financial institutions do have at their behest. For example, most credit card and other financial services companies have anti-fraud mechanisms that identify if and when a customer engages in a transactional pattern that differs from his or her usual pattern. When this happens, the cardholder might receive a call from the institution that issued the card to make sure that the card is indeed being used by the cardholder and not by an unauthorized user. They might ask your mother's maiden name, birth date, or other uniquely private information. The intelligence and law enforcement agencies have come to realize that the same anti-fraud networks that the credit card agencies use can also identify suspicious activity they are interested in. For example, after September 11th, the United States was concerned that a terrorist might use a rented truck to blow up a building. The government might want to know if someone who typically uses a credit card to stay at first-class hotels, purchase first-class airline tickets, and eat at four-star restaurants, suddenly uses his or her cards to rent trucks, stay at motels, and eat at diners. The availability of this information may present an opportunity for intelligence and law enforcement organizations to detect suspicious behavior and activity.

The increasing criminalization of commerce and finance has presented other obstacles. This has been a problem since the advent of bifurcated statutes having both civil and criminal remedies. Banks, government contractors, and other

highly regulated institutions have long had to contend with this. However, since the bright-line distinction between highly regulated institutions and non-regulated institutions has essentially been evaporated, most of industry now has to deal with these same statutes. Of great concern is the loss of scienter in the law: there does not need to be a purposeful action to result in criminal liability.

These bifurcated statutes have created a myriad of interesting questions for financial institutions. For example, last week the U.S. Attorney General announced the indictment of a former professor at a Florida state university for complicity in providing funding to a terrorist institution. What is going to be the obligation of the professor's bank for either having reported or not having reported information to the federal authorities? If there were an act of terrorism tied to this financial activity, what will be the liability of the Florida state banking institution that issued the card to a potentially injured U.S. citizen who then files suit? Those kinds of liability problems are around the corner.

Then, of course, there are the issues of costs and legal privileges. The new regulations and statutes impose great costs upon private business that will eventually be passed onto the consumer. For the lawyers among us, private institutions' providing all this information to the government raises another problem, and that is whether such information is subject to both Federal and State Freedom of Information Acts. For example, Florida's Freedom of Information Act is much broader than the Federal Freedom of Information Act, and the question is whether providing such information to federal or state governmental institutions waives privileges that would otherwise apply to that information? Does providing the information then require a bank or a business to provide that information in general civil litigation? These are the sorts of issues that general counsel offices at companies around the country are grappling with every day as they try and make determinations about what kind of information they should hand over.

There is also the issue of basic technical capability. Companies must be able to store, restore and collate an immense amount of data that they did not have to store before. They will have to develop the capability to restore the information when asked and to collate the information in a meaningful manner. The truth is that most businesses do not have the technical capability to do this.

All of this brings me back full-circle to the fundamental questions I first raised this morning. Assuming business can collect, store, retrieve and then collate all this information, who is going to parse it? Can this parsing be done sufficiently in "real time" to make a difference? Is the regulatory structure being created solving the problems we are facing? For example, as I noted, many of the financial regulatory requirements imposed over the last six months do not and may not necessarily be able to address Internet and other virtual transactions that may not be tied to the identity or nationality of a particular individual. Are we going after the wrong target? These are among the questions we will all need to think about in our efforts to find reasonable solutions in this very difficult environment. Thank you.

* * *